REMARKS/ARGUMENTS

Favorable consideration of this application, as presently amended, is respectfully requested.

Claims 1, 3-10, 12, 14, 15 and 17-25 are pending in the present application. Claims 1, 3, 4, 12, 14, 15 and 21-23 are amended and Claim 2 is cancelled by the present response. Support for amendments to the claims is found in the disclosure as originally filed, at least on page 26, line 26 to page 27, line 2 and page 34, line 25 to page 35, line 6. Thus, no new matter is added.

In the outstanding Action, Claims 21-23 were objected to as including informalities; Claims 1, 5-10, 15, 17-21 and 23-25 were rejected under 35 U.S.C. §103(a) as unpatentable over Newcombe (U.S. Pat. Pub. No. 2003/0172269) in view of Arnold et al. (WO 03/055170, herein "Arnold"); and Claims 2-4, 12, 14 and 22 were rejected under 35 U.S.C. §103(a) as unpatentable over Newcombe and Arnold in further view of Medvinsky (U.S. Pat. Pub. No. 2003/0163693).

With regard to the objection to Claims 21-23 as including informalities, Claims 21-23 have been amended to overcome the objection. Accordingly, Applicants respectfully request that the objection to Claims 21-23 be withdrawn.

Addressing now the rejection of Claims 1, 5-10, 15, 17-21 and 23-25 under 35 U.S.C. §103(a) as unpatentable over Newcombe and Arnold, Applicants respectfully traverse this rejection.

With regard to Claim 1, Applicants respectfully submit that Claim 1 has been amended to incorporate the features of Claim 2.

Amended Claim 1 recites, in part,

> the authentication server which comprises
> authentication means for authenticating a user based on the user authentication information transmitted together with a key information as an authentication request from the user

terminal, the key information representing a public key K_{PU} of the user terminal;

an address allocating means for allocating an address to the user terminal for a successful authentication of the user;

generating means for generating information-for-authentication using at least the allocated address;

a ticket issuing means for issuing a ticket containing the allocated address, the key information which is received from the user terminal and the information-for-authentication;

and a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal;

the user terminal which has a pair of the public key K_{PU} and a private key K_{SU} and comprises:

transmitting means for transmitting the user authentication information and the key information to the authentication server for purpose of an authentication request;

a ticket reception means for receiving the ticket which contains the allocated address, the key information and the information-for-authentication and which is transmitted from the authentication server;

means for setting up the allocated address contained in the ticket as a source address for each packet which is to be transmitted from the user terminal to the application server;

a first session key generating means for calculating a first session secret key which is shared with the application server, from the private key K_{SU} of the user terminal and a public key K_{PS} of the application server;

a packet cryptographic processing means for processing each packet to be transmitted to the application server by the first session secret key to guarantee that there is no forgery in each packet;

means for transmitting a first packet including the ticket to the application server for establishing a session; and

a service request means for transmitting a second packet requesting the service to the application server through the session;

and the application server which has a pair of the public key K_{PS} and a private key K_{SS} and comprises:

a second session key generating means for calculating a second session secret key which is shared with the user terminal, from the private key K_{SS} of the application server and the public key K_{PU} of the user terminal;

a packet verifying means for confirming whether or not each packet received from the user terminal is forged using the second session secret key;

a ticket memory means for storing the ticket transmitted from the user terminal;

ticket verifying means for verifying the presence or absence of any forgery in the information-for-authentication in the ticket transmitted from the user terminal to determine if the

> allocated address contained in the ticket is forged or not and preventing the ticket from being stored in the ticket memory means in the presence of a forgery and further verifying whether or not the key information contained in the ticket in the first packet, which has been verified as not being forged, is the key information representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means;
>
> an address comparison means for determining whether or not the allocated address contained in the ticket which is stored in the ticket memory means coincides with the source address of the second packet which is transmitted from the user terminal through the session; and
>
> a service providing means for transmitting to the user terminal packets which provide the service to the user when a coincidence between the addresses is determined by the address comparison means.

Newcombe describes an authentication server that incorporates local and remote IP addresses received from a client into a ticket and provides the ticket to the client. Furthermore, in Newcombe, the content server compares the IP address in the ticket with the IP address of a packet (source address of the packet) from a client[1] and, if they match, authentication of the client is performed[2] and the content ticket is verified[3] with a content then being sent to the client.[4]

However, Newcombe does not describe or suggest an application server which includes a ticket memory means for storing the ticket transmitted from the user terminal and a ticket verifying means for verifying whether or not the key information contained in the ticket in the first packet is the key information representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means.

The outstanding Action asserts on page 6 that Figure 4 and page 4, paragraph 0056 of Newcombe describes the ticket memory means recited in Claim 1, Applicant respectfully traverse this assertion.

---

[1] See Newcombe, Fig. 12, step 1210.
[2] See Newcombe, Fig. 13, step 1304.
[3] See Newcombe, Fig. 13, step 1306.
[4] See Newcombe, Fig. 13, step 1308.

The authentication data store (ADS) in Fig. 4 of Newcombe is a storage which can be accessed from the authentication server (AS) and the ticket granting server (TGS). That is, the ADS is not included in an application server, nor is such a one that stores a ticket for verifying, in the application server, a source address of every packet from a user terminal. Therefore, the ticket memory means in the present invention differs from the ADS in Newcombe.

As mentioned previously, in Newcombe's system, if the IP address in the ticket matches the IP address of a packet, the application server starts transmission of a content. Once the transmission is started, there would be no further use of the content ticket, which means there would be no need to maintain the content ticket and, therefore, ticket memory means is not provided in Newcombe.

In the claimed invention, the authentication server allocates an address to an authenticated user and provides a ticket containing the allocated address and a key information representing a public key of the user terminal to the user terminal, whereby the user, the allocated address, and the key information are interrelated to each other.

Further, in the claimed invention, upon reception of a ticket from a user terminal, the application server verifies the ticket, and if no forgery is found, the ticket is stored in the ticket memory means. Upon request for content from the user terminal, the source address of the packet is compared to the allocated address in the ticket stored in the ticket memory means, and if they match, the content is transmitted to the user terminal. The ticket memory means is provided so that a source address of every packet from the user terminal can be compared to the allocated address in the ticket stored in the ticket memory means even after having started transmission of the content. This feature is not provided in Newcombe.

In addition, in the claimed invention, it is possible to confirm by verifying the relationship between the key information and the public key of the user terminal using the

ticket verifying means, that a relationship in fact exists between the user terminal with which a session has been established using the public key, and the allocated address which is interrelated to the key information by way of the ticket.

Moreover, if the application server is successful in verifying the relationship between the user terminal and the ticket by comparing the public key of the user terminal which was used to calculate the session secret key with the key information contained in the ticket, it stores the ticket in the ticket memory means, and further compares the source address of every packet from the user terminal with the allocated address in the ticket stored in the ticket memory means to confirm that the packets have certainly been transmitted from the user terminal of an authenticated user. That is, it is possible to confirm the authenticity of the sender of the packets based on the address.

As defined in the amended claim 1, the key information representing the public key of the user terminal is transmitted together with the user authentication information to the authentication server, which in turn incorporates the key information together with the user's allocated address into a ticket and sends it to the user terminal. According to these features, it is possible to guarantee the application server that the authenticated user, the address allocated to the user terminal and the key information are interrelated with each other as explained in paragraph [0052] of the present specification. As a result, it is guaranteed to the application server that the user terminal to which the address in the ticket has been allocated is identical to the counter part user terminal with which a current session has been established using the public key of the user terminal, and that the user of the terminal is identical to the user who has been authenticated by the authentication server, thus achieving a high security.

Moreover, the outstanding Action cites Arnold as curing the deficiencies of Newcombe with regard to the claimed invention.

Arnold describes a system in which a network access server 118 allocates a first IP address to an authenticated user and a server instance (middleware) 110 allocates a second IP address to the user who has accessed the server instance 110 using the first IP address. The server instance 110 serves as a middleware for the user to access e-service providers 100, 102. The server instance 110 neither issues tickets nor receives any information corresponding to the key information.

However, Arnold does not describe or suggest an application server which includes a ticket memory means for storing the ticket transmitted from the user terminal and a ticket verifying means for verifying whether or not the key information contained in the ticket in the first packet is the key information representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means.

Specifically, in amended Claim 1, the authentication server allocates an address to a user terminal, generates a ticket which contains the allocated address and key information, and provides the ticket to the user terminal. The user terminal sends the ticket to an application server, which in turn verifies the ticket and, if no forgery is found, the ticket is stored in a ticket memory means. Thereafter, in response to a request for content from the user terminal, the application server compares the source address of the content requesting packet with the allocated address in the ticket stored in the ticket memory means and, if they match each other, the content is transmitted to the user terminal. This feature is not disclosed by the combination of Newcombe and Arnold.

Medvinsky describes that a public key of a client is sent to KDC (Key Distribution Center which acts as an authentication server). However, in Medvinsky the public key is not sent to the user terminal such that the public key is associated with an allocated address and contained in a ticket. Therefore, it is not possible to verify the relationship between the public key and an address, and it is not possible to guarantee to the application server that a

relationship exists. In addition, in Medvinsky, a public key is sent from a client to KDC so that the public key can be used by the KDC (authentication server) for authentication of a message.

Medvinsky does not describe or suggest an application server which includes a ticket memory means for storing the ticket transmitted from the user terminal and a ticket verifying means for verifying whether or not the key information contained in the ticket in the first packet is the key information representing the public key K_{PU} of the user terminal, and if not, preventing the ticket from being stored in the ticket memory means.

In addition, the outstanding Action has further cited Medvinsky as curing the deficiencies of Newcombe and Arnold with regard to features of the claimed invention.

Specifically, in the claimed invention, the public key establishes a session between the user terminal and the application server, but is not used by the authentication server. That is, the public key of the claimed invention is used differently than the public key described in Medvinsky. In the claimed invention, it is sufficient to send the key information representing the public key of the user terminal instead of sending the public key itself to the authentication server. Further, the key information which is not used by the authentication server is sent to the authentication server so that the key information can be associated with an address when the address is allocated to a user based on authentication. This feature is not taught in Medvinsky.

Moreover with regard to the combination of Newcombe, Arnold and Medvinsky, Applicants respectfully traverse the assertion that it would have been obvious to one of ordinary skill in the art to combine these references. Specifically, in Arnold, the IP address allocated by the server instance establishes a VPN between a user terminal and the server instance. In this connection the IP address is alone used as the authenticator to the e-service provider. The function of allocating an IP address to a user terminal itself is a common

known function performed by various ordinary servers, gateways, routers, and the like, however, prior to the claimed invention, there has never been disclosed a system which performs both address allocation and ticket issuance, or which incorporates the allocated address into the ticket. Thus, even though address allocating devices have been disclosed, nothing in the cited references or any other reference would provide one skilled in the art with sufficient reason to create a system in which a ticket issuing device is provided with a function of allocating addresses and incorporating allocated addresses into tickets.

In Arnold's system, authentication is performed and an IP address is allocated. However, since the system employs a scheme of managing the relationships between authenticated clients and IP addresses through monitoring sessions via a server instance (i.e. the scheme differs from the one which uses tickets as in the claimed invention), it would be unnecessary to issue tickets and, therefore, even for those skilled in the art, there would arise no reason to combine the system of Arnold with that of Newcombe. The server instance in Arnold is intended to provide intermediate services to users for safe connection to e-service providers using VPNs. In Arnold's system, the server instance can monitor and manage clients' accesses via the server instance to e-service providers and the like. As it is described on page 13, lines 3-6 of Arnold, "authentication of any e-service 100, 102 towards the server instance 100 will only require the client's IP-address." Thus, the system of Arnold does not necessitate the use of tickets. Therefore, there would arise no reason to incorporate an allocated address into a ticket.

Thus, Applicants respectfully submit that the combination of Newcombe, Arnold and Medvinsky does not render obvious the features recited in Claim 1, at least, for the reason that this combination does not describe or suggest that:

(1) the authentication server incorporates an address allocated to the user terminal together with the key information into a ticket and provides the ticket to the user terminal;

(2) the application server verifies whether the key information contained in the ticket received from the user terminal is interrelated to the public key of the user terminal which has been used for establishing a session;

(3) if the application server is successful in verification using the ticket, the ticket is stored in the ticket memory means; and

(4) the application server performs verification by comparing the source address of every packet transmitted from the user terminal with the allocated address in the ticket stored in the ticket memory means.

Moreover, with regard to the specific comments included in the response to arguments section on pages 3-4 of the outstanding Action, Applicants have the following response.

Specifically, the outstanding Action states on pages 3-4 that "combining this known teaching [DHCP] into the system of Newcombe is obvious," Applicants respectfully traverse this assertion. The outstanding Action has acknowledged that Newcombe's authentication server does not allocate addresses to user terminals and Arnold's server instance does not issue tickets to clients. Thus, neither Newcombe nor Arnold discloses a server which both allocates addresses and issues tickets. On the other hand, as described in paragraph 0007 of the present specification, in the claimed invention there is provided an advantageous feature of assurance of authenticity of an address using a ticket as a result of the arrangement in which the same authentication server allocates addresses and issues tickets. Since neither Newcombe nor Arnold discloses this claimed feature of guaranteeing authenticity of an address using a ticket, the combination of Newcombe and Arnold cannot render claimed invention obvious.

Newcombe's system and other known ticket protocols such as Kerberos are protocols implemented on an IP network, which pre-requisites that all user terminals be allocated with

an IP address in connection with the network. In Newcombe, an IP address must already be allocated to a client in advance using DHCP, as suggested at page 4, right column, lines 1-5, and only then does the client accesses a ticket issuing server on the IP network to receive a ticket. The features of the system of Arnold would not enhance this process in Newcombe.

Applicants remarks in the previous response did not assert that "the combination of Newcombe and Arnold fail to teach the allocation of the address," but instead asserted that the combination fails to teach allocating an address to a user ***such that a third party (e.g. application server) is assured that the address in the ticket is the one that was originally allocated to the user terminal of the authenticated user.***

In addition, it should be noted that there is a significant difference between a simple address allocation as described by Arnold (DHCP) and the address allocation recited in the claimed invention in which user and allocated address are related to each other. For example, in the case of the system described in Newcombe, let it be supposed that an attack node, generally called a rogue access point, is inserted on a path between a client and an application server where it is possible to access a ticket issuing server. Since the attack node is on the path between the client and the application server, the attack node would be able to determine the client's IP address. The attack node could then authenticate itself to a ticket issuing authentication server using the client's IP address (i.e. IP address spoofing), and obtain a ticket. Even though the authentication is formally valid, e.g. the IP address contained in the ticket originally belonged to the client, the system is nonetheless compromised. In this case, it is not possible for the application server to determine whether the IP address in the ticket has been allocated to the accessing user terminal. Since the IP address in the ticket corresponds with the source address of a packet, the application server would comply with the request for content by the attack node which fabricated the IP address.

In contrast, in the claimed invention, the authentication server authenticates the user for allocation of an address, allocates an address to the user terminal of the authenticated user and incorporates the allocated address and information-for-authentication generated using the allocated address into a ticket and, therefore, it is possible for the application server to determine by verifying the ticket whether or not the address in the ticket has been allocated to a user terminal of an authenticated user by the authentication server.

Moreover, in amended Claim 1, since the ticket contains the allocated address and the key information representing the public key of the user terminal, the user terminal possessing the public key and the address allocated to the user terminal are interrelated to each other by the key information, thus ensuring to the third party (e.g. application server) that the address in the ticket is the one that was allocated to the user terminal of the authenticated user.

Moreover, the outstanding Action asserts on page 4 that "combining known methods which produce predictable results are within the capacities of one skilled in the art." However, Applicants respectfully traverse the assertion that the claimed invention would be predictable. Specifically, Applicants respectfully submit that only with benefit of the disclosure of the present application would the features of the claimed invention be known. No evidence that the claimed invention would be obvious or predictable can be found in the cited references.

In addition the outstanding Action asserts that "Newcombe teaches that the client IP address is the one which is incorporated into the ticket." However, the IP address to be incorporated into the ticket is one that has been presented to the authentication server by the client, but not one that is allocated by the authentication server in response to a request for authentication by the client. As a result, the system of Newcombe discloses that authentication server incorporates into the ticket an IP address which has already been allocated by another server to the client using DHCP.

Further, the outstanding Action asserts that the combination of Newcombe and Arnold "necessitates that the allocated IP be the source address of the client when contacting the content server and it is this address which has to be compared because it is stored within the ticket." As is mentioned above, the system of Arnold does not require issuance of a ticket. In Newcombe's system, the IP address contained in the ticket is one that has been presented from the user terminal as part of a ticket request. Therefore, in Newcombe's system, although the IP address contained in a ticket is an address the user terminal uses, it may not be an address allocated to the user terminal by an authentication server, resulting in that the source address of the packet when connecting to the content server is merely compared to the source address of the packet when requesting the ticket. Hence, this comparison does not satisfy the above mentioned condition necessitated. Further, any comparison using this IP address does not satisfy the above mentioned condition necessitated, and also it does not have any effect similar to that obtainable with the address comparison according to the invention of Claim 1 (the effect of guaranteeing a third party that the IP address has been allocated to the user terminal of an authenticated user).

Moreover, another difference between the claimed invention and the combination of Newcombe and Arnold is that in Claim 1, the application server has two separate processes: one for authenticating the ticket (i.e. verifying whether the address in the ticket coincides with the address allocated to the user terminal of the authenticated user) and storing the ticket, and a second for verifying the source address of every packet from the user terminal in response to the user's request for content (i.e. verifying whether the received packet is the one from the user terminal of the authenticated user). In contrast, in Newcombe, when the address contained in the ticket corresponds to the source address of the packet sender, the content server immediately provides content to the client. Once the transmission of the content is started, the ticket will not be needed anymore and therefore, it is not necessary to

store the ticket. Accordingly, in Newcombe, the content server does not have a function of verifying a source address of every packet from the user terminal. In contrast, in the claimed invention, it is possible to verify the authenticity of the originating user terminal by comparing the source address of every receiving packet with the allocated address in the ticket stored in the ticket memory means.

Accordingly, Applicants respectfully submit that Claim 1 patentably distinguishes over Newcombe, Arnold and Medvinsky considered individually or in combination.

With regard to Claim 7, Applicants respectfully submit that the combination of Newcombe and Arnold does not describe or suggest the claimed reception means which receives from the user terminal an authentication request containing the key information, or the claimed features regarding containing the key information representing the user's public key in the ticket.

Similarly with regard to Claim 15 the combination of Newcombe and Arnold fails to disclose the claimed features. Specifically, Newcombe's content server confirms consistency between the ticket and the packet by comparing the address in the ticket and the source address of the packet before transmitting content. However, once the transmission of the content is started, the content server does not verify the originating user terminal based on address for each packet. In contrast, according to Claim 15, whether the user's allocated address contained in the ticket is forged or not is determined by verifying the information-for-authentication contained in the same ticket, and if the ticket is found not forged, the ticket is stored in the ticket memory means as a genuine ticket, and thereafter, in response to each content request by a user, the application server verifies that the origin of the packets is the user terminal of the authenticated user through comparison between the source address of every packet from the user terminal and the allocated address in the ticket stored in the ticket

memory means. Neither Newcombe nor Arnold discloses such a feature related to the ticket memory means and the use thereof for the address comparison.

Moreover, with regard to Claims 12 and 14, neither Newcombe nor Arnold describes or suggests the feature of the key information generating means or of the user authentication information transmitting means which transmits user authentication information along with the key information to the authentication server.

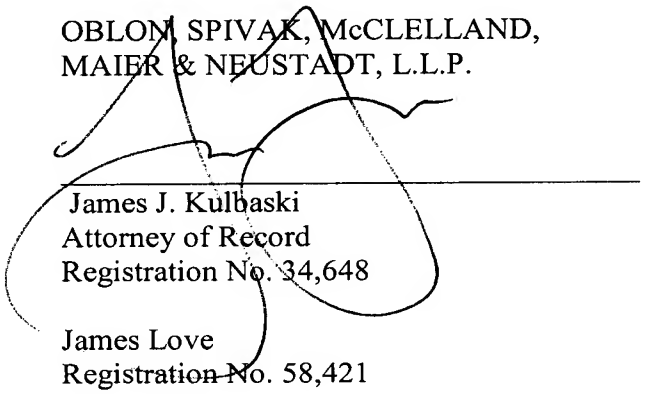
Claims 21-23 recite computer readable medium claims corresponding to the above discussed independent claims.

Accordingly, Applicants respectfully submit that Claims 1, 7, 12, 14, 15 and 21-23, and claims depending respectfully therefrom, patentably distinguish over Newcombe, Arnold and Medvinsky considered individually or in combination.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal allowance. A Notice of Allowance for the claims is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

James Love
Registration No. 58,421

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 07/09)